UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/584,605	05/31/2000	Peter Bendel	DE9-1999-0058	2850

36736 7590 12/14/2005

DUKE W. YEE
YEE & ASSOCIATES, P.C.
P.O. BOX 802333
DALLAS, TX 75380

EXAMINER	
ZIA, SYED	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 12/14/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/584,605	BENDEL ET AL.	
	Examiner	Art Unit	
	Syed Zia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 June 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5,7-9,12-14 and 23-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5,7-9,12-14 and 23-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response filed on June 24, 2005. Original application contained Claims 1-33. Applicant previously cancelled Claims 6, 10-11, and 15-22. Therefore, presently pending claims are 1-5, 7-9, 12-14, and 23-33

2. In view of the Appeal Brief filed on June 24, 2005, PROSECUTION IS HEREBY REOPENED. A new ground of rejection is set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) request reinstatement of the appeal.

If reinstatement of the appeal is requested, such request must be accompanied by a supplemental appeal brief, but no new amendments, affidavits (37 CFR 1.130, 1.131 or 1.132) or other evidence are permitted. See 37 CFR 1.193(b)(2).

Response to Arguments

2. Applicant's arguments with respect to claims 1-5, 7-9, 12-14, and 23-33 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-5, 7-9, 12-14, and 23-33 are rejected under 35 U.S.C. 102(e) as being anticipated by Liao et al. U.S. Patent (6,480,957).

1. Regarding Claim 1 Liao teach and describe a method for controlling access to protected contents on. a server, the method requiring the following components to be present (Fig.1-7): a) a server, b) a client, c) a reader for a mobile security module, d) a security module having at least one protected area for storing a key, e) a data line for communications between client and server (Fig.1, and col.5 line 53 to col. 7 line 12), characterized by the following steps:

aa) sending to the server of a request to call up protected-access contents, bb) sending from the server to the client of an authentication module to be run in the client, cc) execution of an authentication protocol for authenticating the mobile security module and, where appropriate, its holder by means of the authentication module, dd) if the authentication in step cc) was successful, addition to the request in step aa) of a session ID which was generated in the course of the communications between the authentication module and the server, ee) sending of the new request to the server application, ff) checking of the session ID in the request to see that it is recorded in the server, gg) processing of the content requested for transmission and searching of. the contents for further links to other protected-access contents, hh) addition of the session)[D to the links identified, ii) sending of the content modified as in step hh) to the client (Fig.1, 4-7, and col.7 line 13 to line 32, and col.11 line 1 to col.13 line 62).

2. Regarding Claim 23 Liao teach and describe a method, in a client, for controlling access to protected contents (Fig.1-7), the method comprising: sending a request for protected content to a server; receiving an authentication applet and a random number from the server, wherein the random number is generated at the server; executing the authentication applet; sending, by the authentication applet, the random number to a mobile security module, wherein the mobile security module includes a cryptographic key and wherein the mobile security module gencrate3 a cryptographic signature based on the key and the random number; receiving, by the authentication applet, the cryptographic signature from the mobile security module; sending, by the authentication applet, the cryptographic signature to the server; and responsive to the server

authenticating the cryptographic signature, receiving a session identifier from the server Fig.1, 4-7, and col.7 line 13 to line 32, and col.11 line 1 to col.13 line 62).

3. Regarding Claim 27 Liao teach and describe an apparatus, in a client, for controlling access to protected contents (Fig.1-7), the apparatus comprising: means for sending a request for protected content to a server; means for receiving an authentication applet and a random number front the server, wherein the random number is generated at the server; means for executing the authentication applet; means for sending, by the authentication applet, the random number to a mobile security module, wherein the mobile security module includes a cryptographic key and wherein the mobile security module generates a cryptographic signature based on the key and the random number; means for receiving, by the authentication applet, the cryptographic signature from the mobile security module; means for sending, by the authentication. applet, the cryptographic signature to the server; and means for responsive to the server authenticating the cryptographic signature, receiving a session identifier from the server (Fig.1, 4-7, and col.7 line 13 to line 32, and col.11 line 1 to col.13 line 62).

4. Regarding Claim 33 Liao teach and describe a computer program product, in a computer readable medium, for controlling access to protected contents (Fig.1-7), the computer program product comprising: instructions .for sending a request for protected content to a server; instructions for receiving an authentication applet and a random number from the server, wherein the random number is generated at the server; instructions for executing the authentication applet, wherein the applet is configured to perform the following steps: send the random number

to a mobile security module, wherein the mobile security module includes a cryptographic key and wherein the mobile security module generates a cryptographic signature based on the key and the random number; receive the cryptographic signature from the mobile security module; send the cryptographic signature to the server; and responsive to the server authenticating the cryptographic signature, receive a session identifier from the server Fig.1, 4-7, and col.7 line 13 to line 32, and col.11 line 1 to col.13 line 62).

5. Regarding Claims 2-5, 7-9, 12-14, 24-26, and 28-32 are rejected applied as above rejecting Claims 1, 23, 27, and 33. Furthermore, Liao teach and describe a system and method for controlling access to protected contents, wherein:

As per Claim 2, characterized in that the server is a web server and the protected contents are web pages which are called up via a browser by a URL request from a client (col.12line 56 to col.13 line 24).

As per Claim 3, characterized in that the authentication protocol is executed in the followed steps: jj) generation of a random number by the sewer application when the content requested is access-protected and the requirements for access have not been satisfied, and sending of the random number to the authentication module kk) sending of the random number from the authentication module to the mobile security module ll) generation in the mobile security module of a digital signature which takes account of the identity number of the mobile security module, the random number and the key of the mobile security module, mm) sending of

the digital signature to the server, nn) checking of the correctness of tile digital signature using the security module of the server (col.13 line 25 to line 50).

As per Claim 4, characterized in that the server application is a servlet and the client authentication module is an authentication applet and in that on receipt of a URL request the servlet checks the URL request for the presence of a session TD and if there is no session ID present sends an authentication applet containing a random number to the client (col.13 line 51 to line 63).

As per Claim 5, characterized in that the communications between client and server take place via SSL (secure sockets layer) as the transmission protocol (col.5 line 53 to col.6 line 52).

As per Claim 7, characterized in that the digital signature is generated by means of an asymmetrical encryption algorithm with the help of a secret key agreed between client and server, or by means of an asymmetrical encryption algorithm with the help. of a private key, the server being in possession of the public key (col.3 line 36 to line 60, and col.7 line 33 to col.8 line 50).

As per Claim 8, characterized in that the symmetrical encryption algorithm is DES or triple DES and the asymmetrical encryption algorithm is RSA, DSA or an elliptic curve algorithm (col.1 line 63 to col. 2 line 60).

As per Claim 9, characterized in that if the digital signature does not agree, the servlet sends an error message to the client applet (col.12 line 56 to col.13 line 24).

As per Claim 12, characterized in that the session 1D is given a period of validity (col.11 line 1 to line 32).

As per Claim 13, characterized in that the session ID loses its validity on expiry of a fixed time or when a session is terminated by means of a log-off page (col.11 line 1 to line 32).

As per Claim 14, characterized in that the session ID generated in step dd) is recorded in a table and in that the presence of an entry in the table is a requirement for access to all the protected-access pages (col.8 line 52 to col.9 line 30, and col.11 line 34 to col.12 line 55).

As per Claim 24, further comprising: sending a second request for the protected content to the server, wherein the second request includes the session identifier (col. 7 line 34 col.8 line 7).

As per Claim 25, the mobile security module includes an individual number for the mobile security module and wherein the mobile security module generates the cryptographic signature based on the individual number (col.6 line 25 to line 54, and col.7 line 14 to line 62).

As per Claim 26, further comprising: receiving, by the authentication applet, the individual number from the mobile security module; and sending, by the authentication applet, the individual number to the server for authentication (col.6 line 25 to line 54, and col.7 line 34 to line 62).

As per Claim 28, further comprising: means for sending a second request for the protected content to the server, wherein the second request includes the session identifier (col.13 line 51 to line 63).

As per Claim 29, wherein the mobile security module includes an individual number for the mobile security module and wherein the mobile security module generates the cryptographic signature based on the individual number (col.6 line 25 to line 54, and col.7 line 14 to line 62).

As per Claim 30, further comprising: means for receiving, by the authentication applet, the individual number from the mobile security module; and means for sending, by the authentication applet, the individual number to the server for authentication (col.6 line 25 to line 54, and col.7 line 34 to line 62).

As per Claim 31, the mobile security module is a chip card and wherein the client includes a chip card reader (col.6 line 65 to col.7 line 45).

As per Claim 32, the client is a Web client, wherein the server is a Web server, and wherein the protected content is a Web page (col. 12 line 57 to col.13 line 24).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Syed Zia whose telephone number is 571-272-3798. The examiner can normally be reached on 9:00 to 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SZ
November 28, 2005